REMARKS

This Amendment is submitted in response to the Examiner's Action mailed April 14, 2003, with a shortened statutory period of three months set to expire July 14, 2003.

Applicants claim a method, system, and product for securing a transaction in order to prevent fraudulent transactions. Applicants claim the smart card being initialized by a credit card issuer by storing a secret master key and client information on the card. A copy of this master key is also stored within the credit card issuer. The master key is associated with the client information. The master key is kept secret. A digest is created by the smart card using the client information and the master key. This digest is then sent to the credit card issuer in response to the smart card receiving a request for the digest.

The credit card issuer then generates its own digest using the copy of the master key stored by the credit card issuer and the client information. If the digest generated by the credit card issuer matches the digest sent by the merchant, the transaction is authorized.

The Examiner rejected claims 1-2, 5, 7-8, and 11-12 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent 5,850,442 issued to *Muftic*. This rejection is respectfully traversed.

Applicants' claim 1 describes receiving a request for a digest. This is an affirmative step that must be taught in *Muftic* in order for *Muftic* to anticipate Applicants' claims. *Muftic* describes a message digest at column 2, lines 25-51. Nowhere else is *Muftic* are digests discussed. *Muftic* teaches that digests may be created in order to act as an additional verification that data has not been altered since the digest was created. "A message digest of the document is analogous to a cyclic redundancy code (CRC) check sum attached to the end of a packet."

Muftic does not describe, teach, or suggest receiving a request for a digest. As described by the reference, digests are generated and then appended to a document as CRC-type check sums. Requests are not made for the digest itself. The digest is just automatically added as a check sum. *Muftic* does not describe the affirmative step of receiving a request for a digest. Therefore, *Muftic* does not anticipate Applicants' claims.

The Examiner refers to column 2, lines 27-51 and Figure 10, step 1030 as teaching the step of receiving a request for a digest. As discussed above, column 2, lines

27-51 teaches only the existence and typical use of a digest. Column 2, lines 27-52, does not teach receiving a request for a digest. Figure 10, step 1030 describes receiving an order form from a homepage server. Figure 10 describes an order form that is received from a vendor. Figure 10 does not describe the vendor sending a request to a user for a digest. In figure 10, the vendor sends information, not requests for digests.

Applicants' claim 1 also describes the request for the digest being received from a requestor. A master key is received from a third party. A digest is created using unique client information and the master key. The digest and the unique client information are then returned to the requestor. The digest and unique client information will be used for transacting with the third party.

Muftic does not teach returning a digest and unique client information to a requestor that will be used for transacting with the third party that supplied the master key.

Applicants describe retrieving a master key that was received from a third party, and that remains unchanged and kept secret. Applicants' claims describe a copy of the master key being stored by the third party. The Examiner states that *Muftic* teaches retrieving a master key in Figure 10, step 1060. This step of *Muftic's* figure 10 states, "Digitally sign order form, create digital envelope and send to server." The accompanying text, at column 13, lines 36-39, states, "The user digitally signs the order form and sends it to the server or directly to the vendor as specified in information contained on the server (1060)." This section of *Muftic* does not refer to a master key or any other type of key. This section of the reference certainly does not describe a master key that was received from a third party and that remains unchanged and kept secret. This section of the reference does not describe a copy of the master key being stored by the third party.

Applicants' claim 8 describes receiving within a smart a request from a merchant for a billing digest. The Examiner states that the reference describes this step at column 2, lines 15-51 and figure 10, step 1030. Specifically, the Examiner refers to an order form that is received. Applicants, however, do not claim receiving an order form. Applicants claim a smart card that receives a request from a merchant for a billing digest. *Muftic* does not describe, teach, or suggest a smart card that receives a request from a

merchant for a billing digest. *Muftic's* figure 10 describes a user logging on to a home page server, obtaining an order form from the server, filing out the order form, and digitally signing the order form. Nothing in this section of *Muftic*, describes a smart card receiving a request for a digest from a merchant. Figure 10 describes a merchant supplying information to a user. Figure 10 does not describe a merchant sending a request to a user. Figure 10 does not describe a smart card receiving a request from a merchant for a digest.

Applicants' claim 11 similarly describes sending a data transmission to a smart card including unique merchant information and a request for a billing digest. As discussed above, *Muftic* does not describe, teach, or suggest a request for a billing digest.

Applicants' claims describe receiving a secret master key from a third party that remains unchanged and is not altered after the transaction. The third party stores a copy of the master key. *Muftic* teaches public key encryption. However, nothing in *Muftic* explicitly states that a master key is received from a third party that keeps a stored copy where the key remains unchanged and is not altered after the transaction. In public key encryption, typically data is encrypted with one key and decrypted with another. Thus, the decryptor does not have a copy of the key used to encrypt the data.

Muftic does describe a session key that is changed after each transaction. However, this key continually changes. It does not remain unchanged. See column 2, line 63 through column 3, line 2. *Muftic* does not teach a master key that is received from a third party that keeps a stored copy where the key remains unchanged and is not altered after the transaction.

The Examiner rejected claims 3, 6, 9-10, 13-14, 17-26, 28-33, and 36-40 under 35 U.S.C. § 103(a) as being unpatentable over *Muftic*. This rejection is respectfully traversed.

Applicants' claim 3 describes the request for a digest including unique merchant information which is used to access the master key. The Examiner states that it would be obvious to include unique merchant information that would dictate which master key the client system should use. However, this is not what is claimed by Applicants. Applicants claim a request for a digest received from a requestor including unique merchant

information which is used to access a master key that was received from a third party where the third party keeps a copy of the master key.

It is not clear where the merchant information suggested by the Examiner should be included. There is no request for a digest from a requestor in which to include the merchant information. The Examiner had described the request for a digest as being an order form as described by *Muftic's* figure 10, step 1030. This order form is downloaded from a vendor, completed by the user, and then sent back to that same vendor. Thus, the merchant information suggested by the Examiner would be added to an order form that is completed by the user and then supplied back to the merchant. *Muftic* does not describe, teach, or suggest adding merchant information to an order form that was originally retrieved from the merchant, completed, and then supplied back to the merchant. *Muftic* does not provide any teaching as to why a merchant would want to supply merchant information to a user that would then just send that same merchant information back to the merchant.

The Examiner rejected claims 4, 9, 15-16, 27, and 34-35 under 35 U.S.C. § 103(a) as being unpatentable over *Muftic* and further in view of U.S. Patent 5,931,917 issued to *Nguyen*. This rejection is respectfully traversed.

Muftic and *Nguyen* in combination do not describe, teach, or suggest receiving a request for a digest from a requestor where the digest is created using unique client information that includes a reference number provided to a client by a third party.

It is respectfully urged that the subject application is patentable over *Muftic* and *Nguyen*, either singly or in combination, and is now in condition for allowance.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: June 16, 2003

Respectfully submitted,

Lisa Yociss

Lisa L.B. Yociss
Reg. No. 36,975
Carstens, Yee & Cahoon, LLP
P.O. Box 802334
Dallas, TX 75380
(972) 367-2001
ATTORNEY FOR APPLICANTS